AGILEBLUE

Automation. Visibility. Confidence.

Logistics and Transportation Organizations

Whitepaper

AgileBlue, 2021

Overview

The logistics industry is open to cyberattacks just like anyone else. Trucking and logistics companies have suffered their fair share of cyberattacks over the last few years. Imagine losing access to business management technologies all at once. From back-office computer systems, to dispatch, to mobile communications and shop technologies. Continuing to operate as a business would not be possible. Like most organizations, you would pay anything to get your data back. Crippling a business in this way is exactly what cyber criminals are after when they inject ransomware into your systems. Cybersecurity is critically important for logistics and trucking when you consider their environments are automated with components that can be easily compromised for ransom.

Most IT staff admit their toughest challenge is keeping up with threats to the security of their IT systems and data. Cyberattacks are growing in number, intensity, and sophistication. At the same time, the talent that logistic companies need to defend against such threats is becoming harder to find and retain. Forward-looking companies look to utilize more resilient security programs through effectively monitoring and quickly responding to cyber and digital threats.

An outsourced security solution such as a SOC-as-a-Service provides proactive identification, management, and response to cyber and digital security threats. Cybercriminals are now capable of exploiting weaknesses at previously unseen speed and scale by rapidly acquiring new cyber weapons and continuously modifying their attack techniques. As threat actors continue to adapt and evolve, paying attention to cybersecurity strategy is paramount to logistic companies of all sizes.

At a Glance

- The world economic forum indicates that digitalization could unlock business opportunities worth $1.5 trillion for logistic players over the next decade (to 2025).
- According to Gartner, the number of internet-connected devices is expected to reach 50 billion by 2021.
- 38% of logistics companies have significant unresolved questions surrounding data privacy and security (PwC)
- At least 55% of logistics employees feel they are ill-equipped to identify or handle a cyberattack. (The State of Logistics Technology Report)
- Only 21% of logistic companies believe they need to have a CISO (The State of Logistics Technology Report)

Cybersecurity Challenges for Logistics and Transportation

The logistics industry has begun generating large amounts of structured and unstructured data that can be strategically dealt with only by advanced technologies like Internet of Things (IoT) and artificial intelligence. Businesses can achieve greater supply chain transparency and extensively reduce operating expenses by mapping information generated through connected equipment and logistics software to machine learning models implemented in the cloud. When logistic and transportation companies and equipped with IoT solutions, they can monitor goods' whereabouts in real-time and place.

Although the digital transformation within the logistics and transportation industry has proven to be a growing success, it also means that the industry has become an easy target for cyber criminals. With the large number of stakeholders and third-party vendors in the logistics chain, the industry is made extremely vulnerable. SOC-as-a-Service keeps a logistic company's critical infrastructure secure by delivering advanced detection, protection, and automated incident response.

Today's cybercriminals hold a strategic advantage, as they can launch attacks at a fraction of the cost–in terms of time, complexity, and resources–that logistic companies must typically spend to defend against them. The growing numbers of automation, mobile devices and ICS applications further exacerbates the problem in addition to:

- Expanded attack surface: Every endpoint, network device, server, ICS control or application expands the attack surface
- Hostile insiders: Weak or non-existent IT security standards for remote workers often lead to hostile rogue insiders jeopardizing your business
- Human error: Lack of appropriate internal security training and poor supply chain risk management lets even well-intentioned employees or third-party vendors create accidental exposure

Dedicated Security and 24/7 Monitoring to Combat Ransomware and Breach

As digitalization continues to reshape the industry, it's important to invest in security tools and technologies. Like many industries, logistic companies have attempted to meet elements of guidelines by deploying traditional endpoint antivirus (AV) solutions or perimeter defenses like firewalls, assuming these approaches will be enough to make their problems "go away." Unfortunately, these solutions have consistently failed to keep them secure.

It's important that these organizations have complete transparency and visibility to manage risks within their environment.

Here are the top three types of cyberattacks that small and mid-size logistic and transportation companies tend to struggle with, and the reasons why traditional approaches have often failed:

Ransomware is a type of malware that either threatens to block access to a victim's data, publish it, or destroy it unless a ransom in cryptocurrencies is paid. Logistic companies may install AV or endpoint protection platform (EPP) solutions on employee endpoints, but without having an expert team to carefully analyze their alerts and event log data, an attack can go unnoticed. These attacks have become particularly notorious for their ability to evade traditional endpoint controls, leaving most companies vulnerable as they operate without continuous network monitoring capabilities, real-time threat intelligence, or custom threat detection logic.

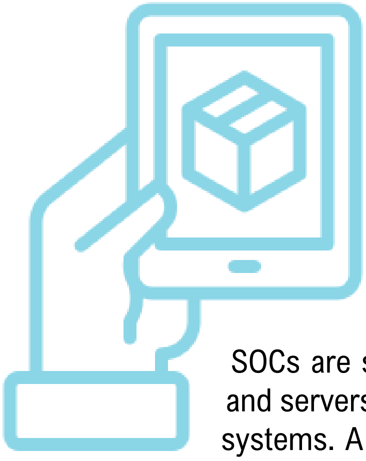
Attacks on unpatched servers and infrastructure are specifically designed to exploit weaknesses and vulnerabilities in servers and other internet-facing systems. In a vast majority of such attacks, patches are publicly announced and made available. For appropriate defense, logistic companies need access to advanced vulnerability scanning tools for system hardening and alerting. Ideally, they should also deploy continuous network monitoring tools with customized rules to detect anomalous scanning requests coming into Internet-facing entities, indicators of attackers probing the system.

Phishing attacks seek to obtain sensitive information such as usernames, passwords, social security numbers or credit card numbers. Attackers typically operate under the guise of a trustworthy entity, such as a reputable third party, or the login page for an email or messaging service. Email security solutions that offer real-time analysis of URLs in emails, email attachments, and web objects can help with detection. But email security solutions are often unable to flag an embedded malicious URL or attachment before the victim interacts with it. In such cases, companies without continuous network monitoring, Active Directory (AD) monitoring, or advanced monitoring for any deployed ICS and SaaS applications are left vulnerable.

A New Approach for a Secure Future: Adopting SOC-as-a-Service

IT teams within the logistics industry only have a few hours to detect an intrusion, investigate the incident, estimate the severity and scope, determine what response actions are necessary, initiate the response, eject the attacker, and contain any damage. Given enough time, attackers can bury themselves deeper, start adapting their moves, and behave like an insider to make it look like whatever they're doing is just regular business activity. This makes detection at a later stage much harder and significantly impacts a company's ability to trace their path during an investigation. This is exactly why logistic companies of all sizes need advanced threat detection and response capabilities with 24x7 security monitoring.

In the aftermath of most data breaches, IT teams find that attacks usually don't look like attacks at all, except in hindsight. Effective detection strategies depend on aggregating and correlating logs from critical components in an organization's network. Detecting patterns of anomalous activity and potential compromise requires the deep analysis of several critical log sources, including:



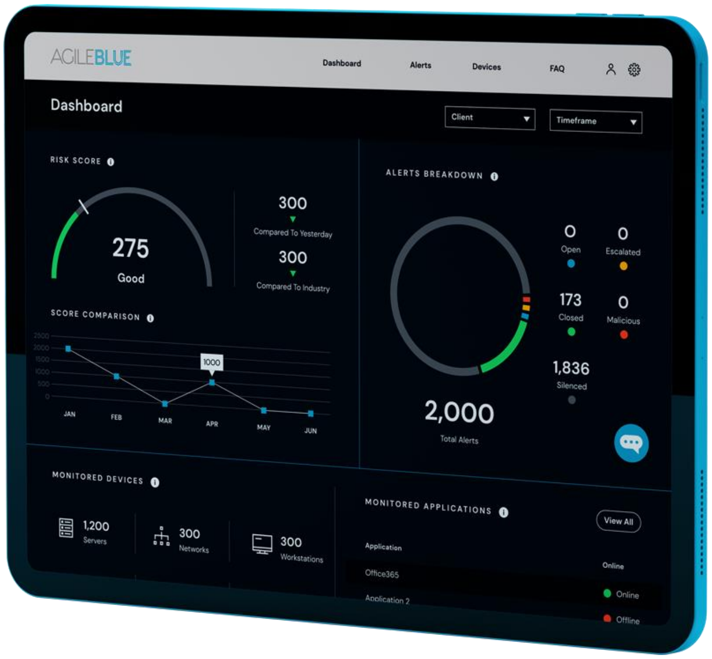
- Firewalls
- IDS/IPS
- Endpoint security (EPP, antivirus)
- Active Directory
- Email security gateways
- SaaS applications
- Cloud workloads

SOCs are staffed with trained security analysts who continuously monitor data centers and servers, user login activity, SaaS applications, cloud workloads, endpoints, and email systems. A SOC enables IT staff to correlate events across multiple, disparate systems, and extract actionable intelligence to aid effective threat detection and response. Unfortunately, its cost is well beyond the budget of most small and mid-sizes organizations. AgileBlue's SOC-as-a-service, delivers the following capabilities at a simple and predictable monthly pricing model– essentially enabling smaller logistic companies to take advantage of security operations. Included are:

- Fully managed, cloud based SIEM
- Machine Learning Engine
- External threat intelligence
- 24x7 monitoring and alerting
- Compliance reporting
- Cloud monitoring–AWS, Azure, Google Cloud
- Periodic external vulnerability scans
- Cyber Risk Score

AgileBlue's Cyber Risk Score

AgileBlue's Cyber Risk Score, pictured below, is a noted differentiator. The Cyber Risk Score is calculated by evaluating the entire landscape of an infrastructure including devices, applications, alerts, behavioral anomalies, best practices, and CVEs (Common Vulnerabilities & Exposures). AgileBlue's proprietary risk scoring algorithm includes 13 different factors that instantly identify vulnerabilities, active exploits, and advanced cyber threats to help rigorously protect a logistic company and strengthen a security posture.



SOC-as-a-Service protects the following from threats so that you can focus on your business:

- IT systems
- Robotics Automation
- ICS controls
- Confidential data

A SOC-as-a-Service enables logistic companies to address the listed security gaps that result in the cyberattacks covered in the prior section going undetected. Using a managed SOC service gives logistic companies complete centralized visibility into their networks' security and the ability to leverage existing point products and security investments. It also creates access to regular vulnerability assessments and enables logistic companies to establish a detailed and customized incident response plan.

What's more, it helps logistic companies provide strong evidence of security processes during control audits, avoid compliance penalties, insurance reviews and establish a new competitive differentiator, thereby increasing competitive differentiation during new business acquisition.

The time for logistic and transportation companies to make strategic security improvements is now. Effective cybersecurity makes organizations more prepared, more resilient, and better protected so that they can continue to fulfill their obligations and represent the needs of their customers.

About AgileBlue

AgileBlue is a managed breach detection company with an Autonomous SOC-as-a-Service for 24x7 monitoring, detection and guided response for cloud, digital infrastructures, and applications. AgileBlue provides their clients with enhanced visibility regarding cyber risk via the AgileBlue analytics reporting dashboard. The company offers a proprietary risk scoring algorithm including industry comparisons and risk analysis trends. AgileBlue's Silencer technology significantly reduces false positives with a 95% confidence score on incident alerts based on their proprietary machine learning and user behavior analytics.

Ready to protect your company? Contact Us.